НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200303.3 | 3 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повреждение кучи в ПО Google Chrome

Идентификатор уязвимости	MITRE: CVE-2020-6407
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код, убедив пользователя посетить специально сформированную HTML-страницу. Уязвимость обусловлена ошибкой определения границ динамической памяти при обработке входящих потоков данных в Google Chrome.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Google Chrome до v80.0.3987.122
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	27 января 2020 г.
Дата обновления	28 февраля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)

Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-6407 https://chromereleases.googleblog.com/2020/02/stable-channel-update-for-desktop_24.html